DRAWINGS

The attached drawing sheets 1-6 including formal drawings for FIGS 1-6, and notated in the top margin as "Replacement Sheet," replaces the original drawing sheets 1-6 including informal drawings. No other amendments of the drawings have been made.

Attachment: Replacement Sheet (see Appendix following page 14).

REMARKS

The application included claims 7, 11-13, 17, 21-27, and 30-38 prior to entering this amendment.

Claims 7, 11-13, 17, 21-27, and 30-38 were rejected.

The Applicant amends claims 7, 11-13, 17, 21, 24-27, 30-32, and 35.

The Applicant adds new claim 39. No new matter is added.

The application remains with claims 7, 11-13, 17, 21-27, and 30-39 after entering this amendment.

Claim Rejections - 35 U.S.C. § 103

The Examiner rejected claims 7, 11, 12, 21, 22, 24, 25, 30, 33, and 38 under 35 U.S.C. § 103(a) over Gupta (U.S. Patent 6,389,532) in view of Shwed (U.S. Patent 5,835,726).

The rejection is traversed in part, however the Applicant amends claims 7, 11, 12, 21, 24, 25, and 30 to expedite prosecution. For example, claim 7 is amended to recite a method, comprising:

> receiving a digital content file for transmission across a distributed computer network, wherein the distributed computer network comprises an intermediate node;
>
> examining data comprising the content file to determine whether the content file includes a restricted data format, the examining performed by the intermediate node within the distributed computer network;
>
> transmitting the content file to a computer system comprising one or more endpoints when data comprising the content file does not include the restricted data format, wherein the computer system is located external to the distributed computer network; and
>
> blocking transmission of the content file when data comprising the content file does include the restricted data format to prevent unauthorized downloading of copyrighted material, wherein the blocking is effected prior to a transmission of the content file to the computer system.

In rejecting claim 7, the Examiner acknowledged that Gupta fails to disclose examining, transmitting, and blocking transmission of the content file. Instead the Examiner suggests that Shwed discloses these features (page 3, first and second paragraphs of the July 9, 2008 Office Action).

Shwed describes a conventional fire wall that filters packets as they flow into or out of a WAN or private network (Abstract). In particular, Shwed identifies that packet filters 204 may each be installed on individual components (i.e. gateways 106 and workstations 104) of the private network (col. 6, lines 3-9 and FIG. 2). Shwed describes the private network as including a main site 100 and a remote site 120 (see FIG. 2). According to Shwed, data flow to or from a particular object of the network can be controlled by use of the packet filters 204, which are "installed on the host device such as the workstation or gateway at which protection is desired (col. 6, lines 10-27). Accordingly, Shwed describes the conventional fire wall and protection techniques provided in Applicant's background section (see page 2, lines 10-19, and page 3, lines 7-16).

The Examiner identified col. 1, lines 40-43, and col. 11, line 66 through col. 12, line 8 of Shwed as allegedly disclosing examining, transmitting and blocking the content file. Even assuming that Shwed's packet filtering process of TCP protocol packets discloses the recited content file including a restricted data format, Applicant respectfully submits that this reference fails to disclose that data comprising the content file is examined by an intermediate node within the distributed computer network, or that the content file is transmitted to a computer system comprising one or more endpoints when data comprising the content file does not include the restricted data format, wherein the computer system is located external to the distributed computer network.

Shwed's packet filters 204 are integrated with the gateways 106 and workstations 104 themselves. In other words, the packet filters 204 (i.e. fire wall) is included as part of Shwed's local or remote sites 100, 120 that comprise his private network. Consistent with this interpretation, Shwed describes that his fire walls 1604, 1608, 2102 (FIGS. 16 and 21) are coupled to the host through a private LAN. As previously argued, Applicant respectfully submits that this is simply conventional fire wall technology wherein the fire wall is established at or with the edge devices or local network.

With respect to the rejection of claims 11 and 24, since the Examiner has already acknowledged that Gupta fails to disclose examining, transmitting, and blocking transmission of the content file, it stands to reason that Gupta would also fail to disclose examining the content file within the distributed computer network, wherein the distributed computer network comprises the Internet. In addition, Applicant respectfully submits that Shwed's packet filters

204 (as well as all of the disclosed routers 110, gateways 106, and workstations 204) are located in either the main site 100 or remote site 120, such that Shwed also fails to disclose examining the content file within the distributed computer network. Applicant points out that Shwed provides absolutely no details for the operation of any nodes within the Internet (FIG. 2) or the public networks (FIGS. 16, 21).

The Examiner has further rejected claims 12 and 25 under Gupta in view of Shwed. Claim 12 recites wherein the examining is performed by one or more routers within the distributed computer network. However, Shwed describes that only the gateways 106 and workstations 204 have installed packet filters 204. Applicant notes that routers 108 (FIG. 1) are illustrated as being connected to reference number 202, however reference number 202 does not appear to be discussed or referenced within the specification to enable one skilled in the art to appreciate what they are. Furthermore, Shwed appears to suggest that the packet filters 204 are incompatible with the routers 208 (col. 5 lines 64-67), such that Applicant respectfully submits that Shwed teaches away from the proposed combination of Gupta and Shwed in rejecting claims 12 and 25.

By way of further example, claim 21 recites, in part, a method comprising:

> examining a digital content file to determine whether the digital content file includes a digital signature, wherein the examining is performed within the distributed computer network;
>
> logging the digital content file and the digital signature to create a file transmission log, wherein the file transmission log is maintained within the distributed computer network; and
>
> identifying a sender of the digital content file according to the digital signature included in the file transmission log after the digital content file has been transmitted, wherein both the sender and the receiver of the digital content file are located external to the distributed computer network.

In rejecting claims 21, 30, and 33, the Examiner cites col. 7, lines 11-27 of Gupta as allegedly disclosing identifying the sender of the digital content file. According to Gupta, the router 104 uses a public key to check the signature 310 of the packet. The signature 310 is decrypted and compared to a fingerprint to determine if the signature 310 is valid. If the signature is valid, the packet is forwarded. Applicant respectfully submits that this section of Gupta would not be understood by one skilled in the art to disclose identifying the sender of the digital content. Rather, Applicant submits that Gupta merely identifies that the signature is valid.

At col. 3, lines 40-47, Gupta states that the fingerprint corresponds to data contained in the packet, and that the encrypted fingerprint is a unique signature which is used to identify that the sender has authorization to send the packet. An identification of the sender's authorization is distinctly different that an identification of the sender. For example, authorization can be identified without also identifying the sender, provided the decrypted signature 310 matches the fingerprint (col. 7, lines 11-27). Gupta fails to disclose why identifying the sender would be desirable in any case, as the point of the system is merely to assure that the packet being multicast is authorized/valid.

Gupta describes that both public and private keys are required to provide secure transmission of the packet (col. 6, lines 8-10). Gupta continues by stating that if there are multiple private keys, an index is associated with each key (col. 6, lines 21-24). By extension, Gupta can therefore be understood to disclose a system wherein each of the authorized senders could use the same public and private key (i.e. no index is associated with the keys). If each of the senders uses the same private key, it follows that the router 104 would not be able to identify the sender according to a digital signature.

The Examiner acknowledges that Gupta fails to disclose logging the digital content file and the digital signature to create a file transmission log, and instead alleges that Shwed discloses these features (page 5 of the Office Action). Specifically, the Examiner cites Figure 5 and reference number 532 of Shwed to disclose the file transmission log of claim 21. According to Shwed, "the packet is compared with the security rule and a determination is made as to whether or not the packet matches the rule. If the packet matches the rule, it may be logged on the system administrator's log." (see col. 9 lines 22-24).

Applicant first notes that the system administrator's log associated with reference number 532 is presumably maintained with the system administrator 102 of FIG. 2 within the main site 100. Accordingly, Shwed fails to disclose a file transmission log maintained within a distributed computer network, as recited by claim 21. Additionally, Applicant respectfully submits that since Gupta fails to disclose identifying a sender, Shwed's log containing packet matches would fail to cure the deficiency of Gupta.

At least for the above reasons, Applicant respectfully requests withdrawal of the rejection of claims 7, 11, 12, 21, 22, 24, 25, 30, 33, and 38.

The Examiner rejected claims 13, 17, 23, 26, 27, 31, 32, and 34-37 under 35 U.S.C. § 103(a) over Gupta in view of Shwed and further in view of Gibbs (U.S. Patent 6,085,321).

The rejection is traversed for similar reasons provided above, as well as for the further novel features recites by claims 13, 17, 23, 26, 27, 31, 32, and 34-37. With respect to the rejection of claims 17, 27, and 31 at page 7 of the Office Action, the Examiner acknowledges that Gupta and Shwed fail to disclose logging the digital content file and digital signature, and instead references Gibbs as allegedly disclosing these features. The rejection is further traversed for reasons stated in Applicant's March 26, 2008 response to the rejection of previously presented claims 17, making specific reference to Gibbs (see page 12 of the March 26, 2008 response).

Accordingly, Applicant respectfully requests withdrawal of the rejection of claims 13, 17, 23, 26, 27, 31, 32, and 34-37.

Applicant notes that the amendment of claims 30 and 31 address an inadvertent error introduced in the prior amendment, wherein the words "includes" and "does not include" have been amended consistent with certain embodiments disclosed in the specification. The error was introduced without deceptive intent.

New Claim

Applicant adds new claim 39 for consideration. No new matter is added.

Any statements made by Examiner that are not addressed by Applicant do not necessarily constitute agreement by the Applicant. In some cases, Applicant may have amended or argued the allowability of independent claims thereby obviating grounds for rejection of the dependent claims.

CONCLUSION

For the foregoing reasons, the Applicant respectfully requests reconsideration and allowance of all pending claims. The Examiner is encouraged to telephone the undersigned if it appears that an interview would be helpful in advancing the case.

Customer No. 73552

Respectfully submitted,

STOLOWITZ FORD COWGER LLP

Bryan Kirkpatrick

Bryan D. Kirkpatrick
Reg. No. 53,135

STOLOWITZ FORD COWGER LLP
621 SW Morrison Street, Suite 600
Portland, OR 97205
(503) 224-2170